bugkuCTF Writeup （Web）41-44

原创

Troublor 于 2018-02-07 20:49:41 发布 1730 收藏 1

分类专栏： CTF 文章标签： CTF Web SQL PHP

这是一个神奇的登陆框

登陆框注入

之前注入的分隔符都用的是单引号`'`，这道题特立独行用的是双引号。
又发现有报错的回显，于是报错注入：
一开始使用的updatexml和extractvalue这两个函数来进行的报错注入，后来发现这两个函数的报错注入有缺陷，报错信息的长度不超过32位，对于这道题来说，flag是一个md5摘要，长度正好32位，而又会用到concat函数来连接，就会显示不完全。
所以这道题的注入还是使用基于`floor()和rand()`的报错注入
payload：

```
admin_name:a1
admin_passwd:1" and (select 1 from (select count(*), concat(floor(rand(0)*2),0x23,(爆数据库信息))x from i
submit:GO GO GO
```

在“爆数据库信息”那里逐个找，就能找到flag1表的flag1字段是flag

多次

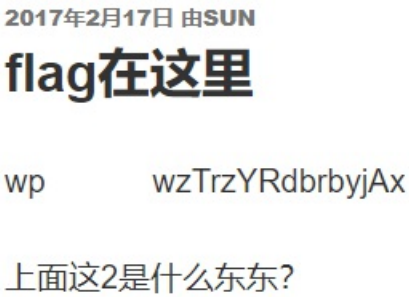
这个暂时还没做出来（忧伤）

sql注入2

自己做没做出来，看别人的，竟然url为`http://120.24.86.145:8007/web2/flag`可以直接下载，无语。
下载下来就是flag。。。

wordpress

信息收集，嗯，就开始扒博客，幸亏文章就一点点，
看到有一个文章说flag在这里，并且下面给了两个字符串



抱着试试看的心态去访问phpmyadmin还成功了，这还真是信息搜集啊
数据库里面很容易就找到flag了

数据库里面很容易就找到flag了